



## Privacy Threshold Analysis

Version number: 01-2014

Page 1 of 12

### PRIVACY THRESHOLD ANALYSIS (PTA)

**This form is used to determine whether  
a Privacy Impact Assessment is required.**

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance  
The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, [www.dhs.gov/privacy](http://www.dhs.gov/privacy), on DHSCconnect and directly from the DHS Privacy Office via email: [pia@hq.dhs.gov](mailto:pia@hq.dhs.gov), phone: 202-343-1717.



## Privacy Threshold Analysis

Version number: 01-2014

Page 2 of 12

### PRIVACY THRESHOLD ANALYSIS (PTA) SUMMARY INFORMATION

<b>Project or Program Name:</b>	ESTA Social Media Tool Pilot Evaluation		
<b>Component:</b>	CBP	<b>Office or Program:</b>	OFO/NTC/TTP
<b>Xacta FISMA Name (if applicable):</b>	Click here to enter text.	<b>Xacta FISMA Number (if applicable):</b>	Click here to enter text.
<b>Type of Project or Program:</b>	Pilot	<b>Project or program status:</b>	Pilot
<b>Date first developed:</b>	June 15, 2016	<b>Pilot launch date:</b>	July 11, 2016
<b>Date of last PTA update</b>	Click here to enter a date.	<b>Pilot end date:</b>	December 31, 2016
<b>ATO Status (if applicable)</b>	Choose an item.	<b>ATO expiration date (if applicable):</b>	Click here to enter a date.

### PROJECT OR PROGRAM MANAGER

<b>Name:</b>	(b) (6), (b) (7)(C)		
<b>Office:</b>	OFO	<b>Title:</b>	Director
<b>Phone:</b>	(b) (6), (b) (7)(C)	<b>Email:</b>	(b) (6), (b) (7)(C)

### INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

<b>Name:</b>	(b) (6), (b) (7)(C)		
<b>Phone:</b>	(b) (6), (b) (7)(C)	<b>Email:</b>	(b)(6)(b)(7)(C)



## SPECIFIC PTA QUESTIONS

### 1. Reason for submitting the PTA: New PTA

The Department of Homeland Security (DHS), U.S. Customs and Border Protection, is responsible for border security while facilitating legitimate travel and trade. CBP has broad authority to vet Electronic System for Travel Authorization (ESTA) applications against various data, including open source and publicly available information derived from social media, to accomplish its border security mission. *See e.g.*, Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53; Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015; Title IV of the Homeland Security Act of 2002, as amended by section 802 of the Trade Facilitation and Trade Enforcement Act of 2015; the Immigration and Naturalization Act, as amended, including 8 U.S.C. 1187(a)(11) and (h)(3), and implementing regulations contained in part 217, title 8, Code of Federal Regulations; the Travel Promotion Act of 2009, Public Law 111-145, 22 U.S.C. 2131; 19 U.S.C. 482, 1467, 1496, 1582, and 1589a.

CBP is entering into a testing and evaluation pilot with the DHS Science and Technology (S&T) Directorate to test and evaluate tools (b) (7)(E) the use of social media for screening and vetting of Electronic System for Travel Authorization (ESTA) applicants. CBP currently accesses publicly available social media, consistent with a previously approved Social Media Operational Use Template (SMOUT), which permits CBP to use (b) (7)(E) techniques (described below) to (b) (7)(E) and vet ESTA applicants. This test and evaluation process does not expand on the types of open source and publicly available information derived from social media information already used by CBP under their inspection authorities.

This initial phase of the pilot project will only cover approximately (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Tools used during the pilot (S&T is in the process of conducting its own PTAs for the Social Media Vetting tools):

1. (b) (7)(E)



2. (b) (7)(E)

For this pilot, information regarding ESTA applicants will be (b) (7)(E) for use by CBP Officers and S&T contracting staff (with CBP officer oversight). All searches and information collected will be done under CBP law enforcement authorities, consistent with the approved SMOUT. S&T contractors will not adjudicate any results. Employees from (b) (7)(E) and supporting contracting staff who are involved in this effort are covered by DHS Non-disclosure agreements (NDA) and terms of the S&T (b) (7)(E) contract. Information provided to (b) (7)(E) for the purposes of expediting searches will be handled in accordance with the DHS NDA and the contract agreement, which requires written certification of data destruction to S&T within two days of destruction of data, and no later than the end of the 30 day period of performance of the contract.

S&T will leverage its contracts to provide (b) (7)(E) to support CBP Officers, if needed. S&T will only use information regarding the process to (b) (7)(E) and will not use any information collected for any operational purposes.

In all cases, CBP will access publicly available information in accordance with its authorities and the privacy policies of the underlying platform. This means that all searches will be conducted using (b) (7)(E) and that CBP Officers must respect individuals' privacy settings and access only information that is publicly available, and cannot "friend, fan, or like" any individuals. Data within (b) (7)(E) is only made available to users in accordance with the privacy policy of the underlying data source. (b) (7)(E).

Information related to the operational experiment will be held in the (b) (7)(E). The S&T Information Systems Security Officer (ISSO) for the HSARPA Data Analytics Laboratory has conducted a preliminary assessment of the (b) (7)(E) security architecture. S&T DA-E ISSO is continuing to assess the security features of the (b) (7)(E). There is a clear boundary between the government system and (b) (7)(E) at the point of query. When the pilot is terminated, data from the pilot will be destroyed (b) (7)(E).

**2. Does this system employ any of the following technologies:**

*If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.*

- ☐ Closed Circuit Television (CCTV)
- ☒ Social Media
- ☐ Web portal<sup>1</sup> (e.g., SharePoint)
- ☐ Contact Lists
- ☐ None of these

<sup>1</sup> Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.



<p><b>3. From whom does the Project or Program collect, maintain, use, or disseminate information?</b></p> <p><i>Please check all that apply.</i></p>	<p><input type="checkbox"/> This program does not collect any personally identifiable information<sup>2</sup></p> <p><input checked="" type="checkbox"/> Members of the public</p> <p><input type="checkbox"/> DHS employees/contractors (list components):</p> <p><input type="checkbox"/> Contractors working on behalf of DHS</p> <p><input type="checkbox"/> Employees of other federal agencies</p>
---	--

<p><b>4. What specific information about individuals is collected, generated or retained?</b></p>
<p>(b)(7)(E)</p>
<p>The full list of ESTA application fields is below:</p> <ul style="list-style-type: none"><li>• Full name (first, middle, and last);</li><li>• Other names or aliases, if available;</li><li>• Date of birth;</li><li>• City and country of birth;</li><li>• Gender;</li><li>• Email address;</li><li>• Telephone number (home, mobile, work, other);</li><li>• Home address (address, apartment number, city, state/region);</li><li>• Internet protocol (IP) address;</li><li>• ESTA application number;</li><li>• Country of residence;</li></ul>

<sup>2</sup> DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.



## Privacy Threshold Analysis

Version number: 01-2014

Page 6 of 12

- Passport number;
- Passport issuing country;
- Passport issuance date;
- Passport expiration date;
- Country of citizenship;
- Other citizenship (country, passport number);
- National identification number, if available;
- Address while visiting the United States (number, street, city, state);
- Emergency point of contact information (name, telephone number, email address); and,
- U.S. Point of Contact (name, address, telephone number).
- Parents' names;
- Current job title;
- Current or previous employer name;
- Current or previous employer street address; and
- Current or previous employer telephone number.

<b>4(a) Does the project, program, or system retrieve information by personal identifier?</b>	(b) (7)(E)
<b>4(b) Does the project, program, or system use Social Security Numbers (SSN)?</b>	(b) (7)(E)
<b>4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:</b>	(b) (7)(E)
<b>4(d) If yes, please describe the uses of the SSNs within the project, program, or system:</b>	(b) (7)(E)
<b>4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure?</b>  <i>For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?</i>	(b) (7)(E)





**4(f) If header or payload data<sup>3</sup> is stored in the communication traffic log, please detail the data elements stored.**

(b) (7)(E)

<p><b>5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems<sup>4</sup>?</b></p>	<p><input type="checkbox"/> No.</p> <p><input checked="" type="checkbox"/> Yes. If yes, please list:</p> <p>PII for ESTA applications is provided by CBP (b) (7)(E) to S&amp;T to facilitate the pilot. (b) (7)(E)</p>
<p><b>6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems<sup>4</sup>?</b></p>	<p><input type="checkbox"/> No.</p> <p><input checked="" type="checkbox"/> Yes. If yes, please list:</p> <p>(b) (7)(E)</p> <p>At the conclusion of the pilot (likely 30-45 days), (b) (7)(E) will destroy all data within 2 days after the pilot has been completed. (b) (7)(E) must certify that all CBP data has been deleted.</p>
<p><b>6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?</b></p>	<p>Existing contract with (b) (7)(E) S&amp;T</p> <p>Please describe applicable information sharing governance in place:</p>
<p><b>7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?</b></p>	<p><input checked="" type="checkbox"/> No.</p> <p><input type="checkbox"/> Yes. If yes, please list:</p>
<p><b>8. -Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to</b></p>	<p><input checked="" type="checkbox"/> No. What steps will be taken to develop and maintain the accounting:</p> <p>CBP, via S&amp;T, is disclosing information to (b) (7)(E) as part of the pilot. However, since (b) (7)(E)</p>

<sup>3</sup> When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

<sup>4</sup> PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.



## Privacy Threshold Analysis

Version number: 01-2014

Page 8 of 12

<b>individuals/agencies who have requested access to their PII?</b>	is under contract with S&T, this is not considered a disclosure under the Privacy Act, but rather a section (m) contractor working on behalf of the agency. No accounting is required. <input type="checkbox"/> Yes. In what format is the accounting maintained:
<b>9. Is there a FIPS 199 determination?<sup>5</sup></b>	<input type="checkbox"/> Unknown. <input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. Please indicate the determinations for each of the following: Confidentiality: <input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined  Integrity: <input checked="" type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined  Availability: <input checked="" type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined

## PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

<b>Component Privacy Office Reviewer:</b>	(b)(6)(b)(7)(C)
<b>Date submitted to Component Privacy Office:</b>	June 21, 2016
<b>Date submitted to DHS Privacy Office:</b>	July 7, 2016
<b>Component Privacy Office Recommendation:</b> <i>Please include recommendation below, including what new privacy compliance documentation is needed.</i>	
The CBP Privacy Office recommends that this joint S&T and CBP pilot is privacy sensitive due to the collection of information from members of the public, namely ESTA applicants and all listed points of contact on the ESTA application, and due to novel privacy compliance issues surrounding the collection of information from social media sites.  No new types of information are collected as part of this pilot, and the test cases being considered have (b)(7)(E) by CBP. (b)(7)(E) (b)(7)(E)	

<sup>5</sup> FIPPS 199 is the [Federal Information Processing Standard](#) Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.





(b) (7)(E) as part of their standard vetting process for ESTA applicants, and do so consistent with the previously adjudicated SMOUT regarding “Analytical Use for Operational Awareness,” which covers users at the National Targeting Center.

Pursuant to the approved SMOUT, CBP Officers may conduct (b)(7)(E) and (b)(7)(E). The ATS PIA references CBP’s use of information on the internet. The CBP Directive on the Operational Use of Social Media, CBP defines (b)(7)(E) and (b)(7)(E) as follows:

- (b)(7)(E)
- (b)(7)(E)

(b) (7)(E)

Therefore, I recommend that this test is covered under the following compliance framework:

1. DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update, June 1, 2012. Per the ATS PIA, ATS maintains the official record “for certain law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information;”
2. DHS/CBP-006 - Automated Targeting System May 22, 2012, 77 FR 30297. Categories of records includes “Operational and analytical reports and/or projects developed that may include public source information and/or classified information obtained by users/analysts for reference or incorporation into the report or project.”

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6)(b)(7)(C)
PCTS Workflow Number:	(b)(6)(b)(7)(C)
Date approved by DHS Privacy Office:	July 8, 2016
PTA Expiration Date	July 8, 2019

DESIGNATION



## Privacy Threshold Analysis

Version number: 01-2014

Page 10 of 12

<b>Privacy Sensitive System:</b>	Yes If "no" PTA adjudication is complete.
<b>Category of System:</b>	IT System If "other" is selected, please describe: Click here to enter text.
<b>Determination:</b>	<input type="checkbox"/> PTA sufficient at this time. <input type="checkbox"/> Privacy compliance documentation determination in progress. <input type="checkbox"/> New information sharing arrangement is required. <input type="checkbox"/> DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. <input type="checkbox"/> Privacy Act Statement required. <input checked="" type="checkbox"/> Privacy Impact Assessment (PIA) required. <input checked="" type="checkbox"/> System of Records Notice (SORN) required. <input type="checkbox"/> Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer. <input type="checkbox"/> A Records Schedule may be required. Contact your component Records Officer.
<b>PIA:</b>	<b>System covered by existing PIA</b> DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update, June 1, 2012
<b>SORN:</b>	<b>System covered by existing SORN</b> DHS/CBP-006 - Automated Targeting System May 22, 2012, 77 FR 30297
<b>DHS Privacy Office Comments:</b> <i>Please describe rationale for privacy compliance determination above.</i>	
<p>The DHS Privacy Office finds that the ESTA Social Media Tool Pilot Evaluation is Privacy Sensitive and requires both PIA and SORN coverage. The pilot, representing a joint effort between U.S. Customs and Border Protection (CBP) and the DHS Science and Technology (S&amp;T) Directorate, involves the testing and evaluation of tools designed (b) (7)(E) the use of social media for the screening and vetting of Electronic System for Travel Authorization (ESTA) applicants. For the purposes of this test, PRIV understands that only the information of individuals that submitted ESTA applications (b) (7)(E) will be used. (b)(7)(E)</p> <p style="text-align: center; font-size: 48pt; font-weight: bold;">(b)(7)(E)</p> <p>The Privacy Office agrees with CBP's assertion that PIA coverage for the ESTA Social Media Tools Pilot is provided under DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update, June 1, 2012, which outlines CBP's use of decision support tools in order to compare traveler information against law enforcement, intelligence, and other enforcement data. Additionally, DHS/CBP/PIA-006(b) outlines the querying of publicly available information on the internet in support of the vetting process. PRIV also</p>	



## Privacy Threshold Analysis

Version number: 01-2014

Page 11 of 12

agrees that SORN coverage falls under DHS/CBP-006 - Automated Targeting System, which notes that CBP collects information on individuals whom may be subject to closer questioning or examination upon arrival to or departure from the United States or who may require further examination, as well as those who may pose a risk to border security or public safety, (b)(7)(E) or may otherwise be engaged in activity in violation of U.S. law. (b) (7)(E)

The update must include the addition of Social Media information to the Categories of Records, as well as publicly available information to the record source.



## **Privacy Threshold Analysis**

**Version number: 01-2014**

*Page 1 of 9*

### **PRIVACY THRESHOLD ANALYSIS (PTA)**

**This form is used to determine whether  
a Privacy Impact Assessment is required.**

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance  
The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, [www.dhs.gov/privacy](http://www.dhs.gov/privacy), on DHSConnect and directly from the DHS Privacy Office via email: [pia@hq.dhs.gov](mailto:pia@hq.dhs.gov), phone: 202-343-1717.



## PRIVACY THRESHOLD ANALYSIS (PTA)

### SUMMARY INFORMATION

<b>Project or Program Name:</b>	ESTA Social Media Tool Pilot Evaluation, Update 1		
<b>Component:</b>	Customs and Border Protection (CBP)	<b>Office or Program:</b>	OFO/NTC/TTP
<b>Xacta FISMA Name (if applicable):</b>	Click here to enter text.	<b>Xacta FISMA Number (if applicable):</b>	Click here to enter text.
<b>Type of Project or Program:</b>	Pilot	<b>Project or program status:</b>	Pilot
<b>Date first developed:</b>	June 15, 2016	<b>Pilot launch date:</b>	July 11, 2016
<b>Date of last PTA update</b>	July 29, 2016	<b>Pilot end date:</b>	December 31, 2017
<b>ATO Status (if applicable)</b>	Choose an item.	<b>ATO expiration date (if applicable):</b>	Click here to enter a date.

### PROJECT OR PROGRAM MANAGER

<b>Name:</b>	<input type="text"/>		
<b>Office:</b>	OFO	<b>Title:</b>	Director
<b>Phone:</b>	<input type="text"/>	<b>Email:</b>	<input type="text"/>

### INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

<b>Name:</b>	<input type="text"/>		
<b>Phone:</b>	<input type="text"/>	<b>Email:</b>	<input type="text"/>





## SPECIFIC PTA QUESTIONS

### 1. Reason for submitting the PTA: Updated PTA

CBP ESTA Social Media Vetting is a pilot project. As a pilot, vetting activities will expand and contract based on new information identified and new areas of interest. This PTA is Update 1 to the ESTA Social Media Tool Pilot Evaluation PTA, adjudicated July 8, 2016.

In an effort to test the capabilities of the social media vetting tools, S&T and CBP seek to look at (b)(7)(E)

(b)(7)(E)

1.

(b)(7)(E)

2.

(b)(7)(E)

### 2. Does this system employ any of the following technologies:

*If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.*

- ☐ Closed Circuit Television (CCTV)  
☒ Social Media



	<input type="checkbox"/> Web portal <sup>1</sup> (e.g., SharePoint) <input type="checkbox"/> Contact Lists <input type="checkbox"/> None of these
--	---

<b>3. From whom does the Project or Program collect, maintain, use, or disseminate information?</b> <i>Please check all that apply.</i>	<input type="checkbox"/> This program does not collect any personally identifiable information <sup>2</sup> <input checked="" type="checkbox"/> Members of the public <input type="checkbox"/> DHS employees/contractors (list components): <input type="checkbox"/> Contractors working on behalf of DHS <input type="checkbox"/> Employees of other federal agencies
--	--

<b>4. What specific information about individuals is collected, generated or retained?</b>
<div style="background-color: black; color: white; text-align: center; padding: 50px;"><h1>(b)(7)(E)</h1></div> <p>The full list of ESTA application fields is below (Stated in the July 8, 2016 PTA):</p> <ul style="list-style-type: none"><li>• Full name (first, middle, and last);</li><li>• Other names or aliases, if available;</li><li>• Date of birth;</li><li>• City and country of birth;</li><li>• Gender;</li><li>• Email address;</li><li>• Telephone number (home, mobile, work, other);</li><li>• Home address (address, apartment number, city, state/region);</li></ul>

<sup>1</sup> Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are “members” of the portal or “potential members” who seek to gain access to the portal.

<sup>2</sup> DHS defines personal information as “Personally Identifiable Information” or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. “Sensitive PII” is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.



- Internet protocol (IP) address;
- ESTA application number;
- Country of residence;

(b)(7)(E)

4(a) Does the project, program, or system retrieve information by personal identifier?

(b)(7)(E)

4(b) Does the project, program, or system use Social Security Numbers (SSN)?

(b)(7)(E)

4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:

[Click here to enter text.](#)

4(d) If yes, please describe the uses of the SSNs within the project, program, or system:

[Click here to enter text.](#)

4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure?

(b)(7)(E)

*For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?*

4(f) If header or payload data<sup>3</sup> is stored in the communication traffic log, please detail the data elements stored.

[Click here to enter text.](#)

<sup>3</sup> When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.



<p>5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems<sup>4</sup>?</p>	<p><input type="checkbox"/> No.</p> <p><input checked="" type="checkbox"/> Yes. If yes, please list:</p> <p>PII for ESTA applications is provided by CBP (b)(7)(E) to S&amp;T to facilitate the pilot. (b)(7)(E)</p> <p>(b)(7)(E)</p>
<p>6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?</p>	<p><input type="checkbox"/> No.</p> <p><input checked="" type="checkbox"/> Yes. If yes, please list:</p> <p>(b)(7)(E)</p> <p>(b)(7)(E) At the conclusion of the pilot (likely 30-45 days), (b)(7)(E) will destroy all data within 2 days after the pilot has been completed. (b)(7)(E) must certify that all CBP data has been deleted.</p>
<p>6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?</p>	<p>Existing</p> <p>Please describe applicable information sharing governance in place:</p>
<p>7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?</p>	<p><input checked="" type="checkbox"/> No.</p> <p><input type="checkbox"/> Yes. If yes, please list:</p>
<p>8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals/agencies who have requested access to their PII?</p>	<p><input checked="" type="checkbox"/> No. What steps will be taken to develop and maintain the accounting:</p> <p>CBP, via S&amp;T, is disclosing information to (b)(7)(E) as part of the pilot. However, since (b)(7)(E) is under contract with S&amp;T, this is not considered a disclosure under the Privacy Act, but rather a section (m) contractor working on behalf of the agency. No accounting is required.</p>

<sup>4</sup> PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.



## Privacy Threshold Analysis

Version number: 01-2014

Page 7 of 9

	<input type="checkbox"/> Yes. In what format is the accounting maintained:
<b>9. Is there a FIPS 199 determination?<sup>4</sup></b>	<input type="checkbox"/> Unknown. <input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. Please indicate the determinations for each of the following:  Confidentiality: <input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined  Integrity: <input checked="" type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined  Availability: <input checked="" type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined

## PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

<b>Component Privacy Office Reviewer:</b>	(b)(6)(b)(7)(C)
<b>Date submitted to Component Privacy Office:</b>	July 29, 2016
<b>Date submitted to DHS Privacy Office:</b>	August 2, 2016
<b>Component Privacy Office Recommendation:</b> <i>Please include recommendation below, including what new privacy compliance documentation is needed.</i>	
The CBP Privacy Office recommends that this joint S&T and CBP pilot is privacy sensitive due to the collection of information from members of the public, namely ESTA applicants and all listed points of contact on the ESTA application, and due to novel privacy compliance issues surrounding the collection of information from social media sites.  The recommendations I provided in the July 8, 2016 PTA apply to this Update 1 as well.	

<sup>4</sup> FIPS 199 is the [Federal Information Processing Standard](#) Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.





## Privacy Threshold Analysis

Version number: 01-2014

Page 8 of 9

For coverage, I recommend that this test is covered under the following compliance framework:

1. DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update, June 1, 2012. Per the ATS PIA, ATS maintains the official record “for certain law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information;”
2. DHS/CBP-006 - Automated Targeting System May 22, 2012, 77 FR 30297. Categories of records includes “Operational and analytical reports and/or projects developed that may include public source information and/or classified information obtained by users/analysts for reference or incorporation into the report or project.”

### (TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6)(b)(7)(C)
PCTS Workflow Number:	(b)(6)(b)(7)(C)
Date approved by DHS Privacy Office:	August 19, 2016
PTA Expiration Date	December 31, 2017 or the end of this pilot, whichever comes first.

### DESIGNATION

Privacy Sensitive System:	Yes If “no” PTA adjudication is complete.
Category of System:	IT System If “other” is selected, please describe: Click here to enter text.
Determination:	<div><input type="checkbox"/> PTA sufficient at this time. <input type="checkbox"/> Privacy compliance documentation determination in progress. <input type="checkbox"/> New information sharing arrangement is required. <input type="checkbox"/> DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. <input type="checkbox"/> Privacy Act Statement required. <input checked="" type="checkbox"/> Privacy Impact Assessment (PIA) required. <input checked="" type="checkbox"/> System of Records Notice (SORN) required. <input type="checkbox"/> Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer.</div>



## Privacy Threshold Analysis

Version number: 01-2014

Page 9 of 9

<input type="checkbox"/> A Records Schedule may be required. Contact your component Records Officer.	
<b>PIA:</b>	<b>System covered by existing PIA</b> If covered by existing PIA, please list: DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update, June 1, 2012
<b>SORN:</b>	<b>System covered by existing SORN</b> If covered by existing SORN, please list: DHS/CBP-006 - Automated Targeting System May 22, 2012, 77 FR 30297
<b>DHS Privacy Office Comments:</b> <i>Please describe rationale for privacy compliance determination above.</i>	
CBP and S&T are (b)(7)(E) (b)(7)(E) PRIV finds that this pilot continues to receive coverage under the ATS PIA and SORN. (b)(7)(E)	
(b)(7)(E)	
(b)(7)(E) The update must include the addition of Social Media information to the Categories of Records, as well as publicly available information to the record source.	



## **Privacy Threshold Analysis**

**Version number: 01-2014**

*Page 1 of 10*

### **PRIVACY THRESHOLD ANALYSIS (PTA)**

**This form is used to determine whether  
a Privacy Impact Assessment is required.**

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance  
The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, [www.dhs.gov/privacy](http://www.dhs.gov/privacy), on DHSConnect and directly from the DHS Privacy Office via email: [pia@hq.dhs.gov](mailto:pia@hq.dhs.gov), phone: 202-343-1717.



## PRIVACY THRESHOLD ANALYSIS (PTA)

### SUMMARY INFORMATION

<b>Project or Program Name:</b>	ESTA Social Media Tool Pilot Evaluation, Update 2		
<b>Component:</b>	Science and Technology (S&T)	<b>Office or Program:</b>	HSARPA
<b>Xacta FISMA Name (if applicable):</b>	Click here to enter text.	<b>Xacta FISMA Number (if applicable):</b>	Click here to enter text.
<b>Type of Project or Program:</b>	Pilot	<b>Project or program status:</b>	Pilot
<b>Date first developed:</b>	June 15, 2016	<b>Pilot launch date:</b>	July 11, 2016
<b>Date of last PTA update</b>	July 29, 2016	<b>Pilot end date:</b>	December 31, 2017
<b>ATO Status (if applicable)</b>	Choose an item.	<b>ATO expiration date (if applicable):</b>	Click here to enter a date.

### PROJECT OR PROGRAM MANAGER

<b>Name:</b>	(b)(6)(b)(7)(C)		
<b>Office:</b>	HSARPA	<b>Title:</b>	Director, DA-E
<b>Phone:</b>	(b)(6)(b)(7)(C)	<b>Email:</b>	(b)(6)(b)(7)(C)

### INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

<b>Name:</b>	(b)(6)(b)(7)(C)		
<b>Phone:</b>	(b)(6)(b)(7)(C)	<b>Email:</b>	(b)(6)(b)(7)(C)



## SPECIFIC PTA QUESTIONS

### 1. Reason for submitting the PTA: Updated PTA

This update includes piloting of new tools, in addition to (b)(7)(E) which has been used to-date. S&T continues to test open source and social media tools for the Department. S&T and CBP may jointly test other tools identified by S&T's assessment of over 275 social media tools. The assessment will continually be updated to identify new capabilities for DHS. The rules and understanding established by this PTA will apply to the piloting of the other tools. Potential tools include:

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

- (b)(7)(E)
- 
- 
- 
- 
- 
- 
- 

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)





(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

**2. Does this system employ any of the following technologies:**

*If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.*

- ☐ Closed Circuit Television (CCTV)
- ☒ Social Media
- ☐ Web portal<sup>1</sup> (e.g., SharePoint)
- ☐ Contact Lists
- ☐ None of these

**3. From whom does the Project or Program collect, maintain, use, or disseminate information?**

- ☐ This program does not collect any personally identifiable information<sup>2</sup>

<sup>1</sup> Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are “members” of the portal or “potential members” who seek to gain access to the portal.

<sup>2</sup> DHS defines personal information as “Personally Identifiable Information” or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. “Sensitive PII” is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.



<i>Please check all that apply.</i>	<input checked="" type="checkbox"/> Members of the public <input type="checkbox"/> DHS employees/contractors (list components): <input type="checkbox"/> Contractors working on behalf of DHS <input type="checkbox"/> Employees of other federal agencies
-------------------------------------	---

#### 4. What specific information about individuals is collected, generated or retained?

The Social Media tools are being tested using ESTA data.

(b)(7)(E)

The full list of ESTA application fields is below (Stated in the July 8, 2016 PTA and updated to reflect the request for applicants' social media accounts, if approved):

- Full name (first, middle, and last);
- Other names or aliases, if available;
- Date of birth;
- City and country of birth;
- Gender;
- Email address;
- Telephone number (home, mobile, work, other);
- Home address (address, apartment number, city, state/region);
- Internet protocol (IP) address;
- ESTA application number;
- Country of residence;
- Social media handles

(b)(7)(E)



<b>4(a) Does the project, program, or system retrieve information by personal identifier?</b>	(b)(7)(E)
<b>4(b) Does the project, program, or system use Social Security Numbers (SSN)?</b>	(b)(7)(E)
<b>4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:</b>	Click here to enter text.
<b>4(d) If yes, please describe the uses of the SSNs within the project, program, or system:</b>	Click here to enter text.
<b>4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure?</b>  <i>For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?</i>	(b)(7)(E)
<b>4(f) If header or payload data<sup>3</sup> is stored in the communication traffic log, please detail the data elements stored.</b>	
Click here to enter text.	

<b>5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems<sup>4</sup>?</b>	<input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. If yes, please list: For the initial pilot that ended September 9, 2016, PII for ESTA applications was provided by CBP (b)(7)(E) to S&T to facilitate the pilot. (b)(7)(E) (b)(7)(E)
--	---

<sup>3</sup> When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

<sup>4</sup> PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.



	<b>(b)(7)(E)</b>
<b>6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?</b>	<input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. If yes, please list: <b>(b)(7)(E)</b> <b>(b)(7)(E)</b> At the conclusion of the operational pilot (likely 6 months), <b>(b)(7)(E)</b> will destroy all data within 2 days after the pilot has been completed. <b>(b)(7)(E)</b> must certify that all CBP data has been deleted.
<b>6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?</b>	Existing Please describe applicable information sharing governance in place:
<b>7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?</b>	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please list:
<b>8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals/agencies who have requested access to their PII?</b>	<input checked="" type="checkbox"/> No. What steps will be taken to develop and maintain the accounting: CBP and S&T are disclosing information to <b>(b)(7)(E)</b> as part of the pilot. However, since <b>(b)(7)(E)</b> is under contract with S&T, this is not considered a disclosure under the Privacy Act, but rather a section (m) contractor working on behalf of the agency. No additional accounting is required.  <input type="checkbox"/> Yes. In what format is the accounting maintained:
<b>9. Is there a FIPS 199 determination?<sup>4</sup></b>	<input type="checkbox"/> Unknown.

<sup>4</sup> FIPS 199 is the [Federal Information Processing Standard](#) Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.



## Privacy Threshold Analysis

Version number: 01-2014

Page 8 of 10

	<input type="checkbox"/> No.
	<input checked="" type="checkbox"/> Yes. Please indicate the determinations for each of the following:
	Confidentiality: <input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined
	Integrity: <input checked="" type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined
	Availability: <input checked="" type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined

## PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

<b>Component Privacy Office Reviewer:</b>	(b)(6)(b)(7)(C)
<b>Date submitted to Component Privacy Office:</b>	July 29, 2016
<b>Date submitted to DHS Privacy Office:</b>	November 15, 2016
<b>Component Privacy Office Recommendation:</b> <i>Please include recommendation below, including what new privacy compliance documentation is needed.</i>	
The S&T Privacy Office recommends these activities be covered under:  1) DHS-S&T-PIA-027, DHS S&T Test Data PIA  2) DHS/S&T-001 Research, Development, Test, and Evaluation System of Records  S&T will use CBP data for test and evaluation only. S&T will not take any operational actions from the results of the tools tested.  The CBP Privacy Office recommends that this joint S&T and CBP pilot is privacy sensitive due to the collection of information from members of the public, namely ESTA applicants and all listed points of contact on the ESTA application, and due to novel privacy compliance issues surrounding the collection of information from social media sites.	





The recommendations I provided in the July 8, 2016 PTA apply to this Update 2 as well.

For coverage, I recommend that this test is covered under the following compliance framework:

The ESTA applicant information is covered under the ESTA PIA and SORN:

1. DHS/CBP/PIA-007(g) Electronic System for Travel Authorization (ESTA) Update, September 1, 2016. Per the ESTA PIA, the ESTA application questionnaire was enhanced, including the addition of an optional field for social media usernames or identifiers for all ESTA applicants.
2. DHS/CBP-009 – Electronic System for Travel Authorization September 2, 2016, 81 FR 60713. Categories of records include “Social media identifiers, such as username(s) and platforms used” and “Publicly available information from social media Web sites or platforms”.

Any additional data (b)(7)(E) from publicly available social media is covered under ATS:

1. DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update, June 1, 2012. Per the ATS PIA, ATS maintains the official record “for certain law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information;”
2. DHS/CBP-006 - Automated Targeting System May 22, 2012, 77 FR 30297. Categories of records includes “Operational and analytical reports and/or projects developed that may include public source information and/or classified information obtained by users/analysts for reference or incorporation into the report or project.”

**(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)**

<b>DHS Privacy Office Reviewer:</b>	(b)(6)(b)(7)(C)
<b>PCTS Workflow Number:</b>	(b)(6)(b)(7)(C)
<b>Date approved by DHS Privacy Office:</b>	November 21, 2016
<b>PTA Expiration Date</b>	December 31, 2017

**DESIGNATION**

<b>Privacy Sensitive System:</b>	Yes If “no” PTA adjudication is complete.
<b>Category of System:</b>	IT System If “other” is selected, please describe: Click here to enter text.
<b>Determination:</b>	<input type="checkbox"/> PTA sufficient at this time. <input type="checkbox"/> Privacy compliance documentation determination in progress.



## Privacy Threshold Analysis

Version number: 01-2014

Page 10 of 10

<input type="checkbox"/> New information sharing arrangement is required. <input type="checkbox"/> DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. <input type="checkbox"/> Privacy Act Statement required. <input checked="" type="checkbox"/> Privacy Impact Assessment (PIA) required. <input checked="" type="checkbox"/> System of Records Notice (SORN) required. <input type="checkbox"/> Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer. <input type="checkbox"/> A Records Schedule may be required. Contact your component Records Officer.	
<b>PIA:</b>	<b>New PIA is required.</b> If covered by existing PIA, please list: New Social Media Vetting PIA
<b>SORN:</b>	System covered by existing SORN If covered by existing SORN, please list: DHS/S&T-001 Research, Development, Test, and Evaluation Records, January 15, 2013, 78 FR 3019
<b>DHS Privacy Office Comments:</b> <i>Please describe rationale for privacy compliance determination above.</i>	
<p>S&amp;T is submitting the PTA to discuss the piloting of new tools, in addition to (b)(7)(E) which has been used to-date. S&amp;T continues to test (b)(7)(E) and social media tools for the Department. S&amp;T and CBP may jointly test other tools identified by S&amp;T's assessment of over 275 social media tools.</p> <p>PRIV finds that is a privacy sensitive system and a PIA is required because S&amp;T collects PII from members of the public.</p> <p>PRIV finds that the forthcoming S&amp;T Social Media Vetting PIA will provide coverage. Social Media Vetting PIA will discuss the social media tools developed by S&amp;T as well as the limited amount of social media data collected and used to conduct research, development, testing and evaluation in support of federal, state, local and tribal, first responder, and law enforcement needs.</p> <p>PRIV finds that a SORN is required because S&amp;T retrieves information by a unique identifier. S&amp;T has said it will use CBP data for test and evaluation only, therefore, PRIV agrees with S&amp;T that the Research, Development, Test, and Evaluation SORN adequately provides coverage. DHS/S&amp;T-001 covers records that are collected for the purpose of furthering S&amp;T's mission to push innovation and development, and the use of high technology in support of homeland security.</p> <p>This phase of this pilot may include other social media tools. S&amp;T is required to update the tool-specific PTA for any of these tools or new tools added that are planned to be used. This PTA expires at the end of the pilot on December 31, 2017.</p>	



## **Privacy Threshold Analysis**

**Version number: 01-2014**

*Page 1 of 11*

### **PRIVACY THRESHOLD ANALYSIS (PTA)**

**This form is used to determine whether  
a Privacy Impact Assessment is required.**

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance  
The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, [www.dhs.gov/privacy](http://www.dhs.gov/privacy), on DHSConnect and directly from the DHS Privacy Office via email: [pia@hq.dhs.gov](mailto:pia@hq.dhs.gov), phone: 202-343-1717.



## PRIVACY THRESHOLD ANALYSIS (PTA)

### SUMMARY INFORMATION

<b>Project or Program Name:</b>	ESTA Social Media Tool Pilot Evaluation, Update 2		
<b>Component:</b>	Customs and Border Protection (CBP)	<b>Office or Program:</b>	OFO/NTC/TTP
<b>Xacta FISMA Name (if applicable):</b>	Click here to enter text.	<b>Xacta FISMA Number (if applicable):</b>	Click here to enter text.
<b>Type of Project or Program:</b>	Pilot	<b>Project or program status:</b>	Pilot
<b>Date first developed:</b>	June 15, 2016	<b>Pilot launch date:</b>	July 11, 2016
<b>Date of last PTA update</b>	July 29, 2016	<b>Pilot end date:</b>	December 31, 2017
<b>ATO Status (if applicable)</b>	Choose an item.	<b>ATO expiration date (if applicable):</b>	Click here to enter a date.

### PROJECT OR PROGRAM MANAGER

<b>Name:</b>	(b)(6)(b)(7)(C)		
<b>Office:</b>	OFO	<b>Title:</b>	Director
<b>Phone:</b>	(b)(6)(b)(7)(C)	<b>Email:</b>	(b)(6)(b)(7)(C)

### INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

<b>Name:</b>	(b)(6)(b)(7)(C)		
<b>Phone:</b>	(b)(6)(b)(7)(C)	<b>Email:</b>	(b)(6)(b)(7)(C)



## SPECIFIC PTA QUESTIONS

### 1. Reason for submitting the PTA: Updated PTA

CBP ESTA Social Media Vetting is a pilot project. As a pilot, vetting activities will be fluid to allow for a range of information to be researched. This PTA is Update 2 to the ESTA Social Media Tool Pilot Evaluation PTA, adjudicated July 8, 2016.

(b)(7)(E)

1.

(b)(7)(E)

2.

(b)(7)(E)

This update also includes piloting of new tools, in addition to (b)(7)(E) which has been used to-date. S&T continues to test (b)(7)(E) and social media tools for the Department. S&T and CBP may jointly test other tools identified by S&T's assessment of over 275 social media tools. The assessment will continually be updated to identify new capabilities for DHS. The rules and understanding established by this PTA will apply to the piloting of the other tools. Potential tools include:

(b)(7)(E)

(b)(7)(E)



(b)(7)(E)

(b)(7)(E)

- (b)(7)(E)
- 
- 
- 
- 
- 
- 
- 
- 

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)





(b)(7)(E)

In all cases, CBP will access publicly available information in accordance with its authorities and the privacy policies of the underlying platform. This means that all searches will be conducted using (b)(7)(E) and that CBP Officers must respect individuals' privacy settings and access only information that is publicly available, and cannot "friend, fan, or like" any individuals. Data within the social media tools is only made available to users in accordance with the privacy policy of the underlying data source.

**2. Does this system employ any of the following technologies:**

*If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.*

- ☐ Closed Circuit Television (CCTV)
- ☒ Social Media
- ☐ Web portal<sup>1</sup> (e.g., SharePoint)
- ☐ Contact Lists
- ☐ None of these

**3. From whom does the Project or Program collect, maintain, use, or disseminate information?**

*Please check all that apply.*

- ☐ This program does not collect any personally identifiable information<sup>2</sup>
- ☒ Members of the public
- ☐ DHS employees/contractors (list components):
- ☐ Contractors working on behalf of DHS
- ☐ Employees of other federal agencies

<sup>1</sup> Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.

<sup>2</sup> DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.



#### 4. What specific information about individuals is collected, generated or retained?

(b)(7)(E)

The full list of ESTA application fields is below (Stated in the July 8, 2016 PTA and updated to reflect the request for applicants' social media accounts, if approved):

- Full name (first, middle, and last);
- Other names or aliases, if available;
- Date of birth;
- City and country of birth;
- Gender;
- Email address;
- Telephone number (home, mobile, work, other);
- Home address (address, apartment number, city, state/region);
- Internet protocol (IP) address;
- ESTA application number;
- Country of residence;
- Social media handles

(b)(7)(E)

4(a) Does the project, program, or system retrieve information by personal identifier?

(b)(7)(E)

4(b) Does the project, program, or system use Social Security Numbers (SSN)?

(b)(7)(E)

4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:

[Click here to enter text.](#)



<b>4(d) If yes, please describe the uses of the SSNs within the project, program, or system:</b>	Click here to enter text.
<b>4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure?</b>  <i>For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?</i>	(b)(7)(E)
<b>4(f) If header or payload data<sup>3</sup> is stored in the communication traffic log, please detail the data elements stored.</b>	
Click here to enter text.	

<b>5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems<sup>4</sup>?</b>	<input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. If yes, please list: For the initial pilot that ended September 9, 2016, PII for ESTA applications was provided by CBP (b)(7)(E) to S&T to facilitate the pilot. (b)(7)(E) (b)(7)(E) (b)(7)(E)
<b>6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?</b>	<input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. If yes, please list: (b)(7)(E) (b)(7)(E) At the conclusion of the operational pilot (likely 6 months). (b)(7)(E)

<sup>3</sup> When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

<sup>4</sup> PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.



## Privacy Threshold Analysis

Version number: 01-2014

Page 8 of 11

	(b)(7)(E) will destroy all data within 2 days after the pilot has been completed. (b)(7)(E) must certify that all CBP data has been deleted.
6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	Existing Please describe applicable information sharing governance in place:
7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please list:
8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals/agencies who have requested access to their PII?	<input checked="" type="checkbox"/> No. What steps will be taken to develop and maintain the accounting: CBP and S&T are disclosing information to (b)(7)(E) as part of the pilot. However, since (b)(7)(E) is under contract with S&T, this is not considered a disclosure under the Privacy Act, but rather a section (m) contractor working on behalf of the agency. No additional accounting is required.  <input type="checkbox"/> Yes. In what format is the accounting maintained:
9. Is there a FIPS 199 determination? <sup>4</sup>	<input type="checkbox"/> Unknown. <input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. Please indicate the determinations for each of the following:  Confidentiality: <input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined  Integrity: <input checked="" type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined  Availability:

<sup>4</sup> FIPS 199 is the [Federal Information Processing Standard](#) Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.



	<input checked="" type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined
--	--

## PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

<b>Component Privacy Office Reviewer:</b>	(b)(6)(b)(7)(C)
<b>Date submitted to Component Privacy Office:</b>	July 29, 2016
<b>Date submitted to DHS Privacy Office:</b>	August 2, 2016
<b>Component Privacy Office Recommendation:</b> <i>Please include recommendation below, including what new privacy compliance documentation is needed.</i>	
<p>The CBP Privacy Office recommends that this joint S&amp;T and CBP pilot is privacy sensitive due to the collection of information from members of the public, namely ESTA applicants and all listed points of contact on the ESTA application, and due to novel privacy compliance issues surrounding the collection of information from social media sites.</p> <p>The recommendations I provided in the July 8, 2016 PTA apply to this Update 2 as well.</p> <p>For coverage, I recommend that this test is covered under the following compliance framework:</p> <p>The ESTA applicant information is covered under the ESTA PIA and SORN:</p> <ol style="list-style-type: none"><li>1. DHS/CBP/PIA-007(g) Electronic System for Travel Authorization (ESTA) Update, September 1, 2016. Per the ESTA PIA, the ESTA application questionnaire was enhanced, including the addition of an optional field for social media usernames or identifiers for all ESTA applicants.</li><li>2. DHS/CBP-009 – Electronic System for Travel Authorization September 2, 2016, 81 FR 60713. Categories of records include “Social media identifiers, such as username(s) and platforms used” and “Publicly available information from social media Web sites or platforms”.</li></ol> <p>Any additional data (b)(7)(E) from publicly available social media is covered under ATS:</p> <ol style="list-style-type: none"><li>1. DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update, June 1, 2012. Per the ATS PIA, ATS maintains the official record “for certain law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information;”</li><li>2. DHS/CBP-006 - Automated Targeting System May 22, 2012, 77 FR 30297. Categories of records includes “Operational and analytical reports and/or projects developed that may include</li></ol>	





public source information and/or classified information obtained by users/analysts for reference or incorporation into the report or project.”

**(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)**

<b>DHS Privacy Office Reviewer:</b>	(b)(6)(b)(7)(C)
<b>PCTS Workflow Number:</b>	(b)(6)(b)(7)(C)
<b>Date approved by DHS Privacy Office:</b>	November 21, 2016
<b>PTA Expiration Date</b>	December 31, 2017

**DESIGNATION**

<b>Privacy Sensitive System:</b>	Yes If “no” PTA adjudication is complete.
<b>Category of System:</b>	IT System If “other” is selected, please describe: Click here to enter text.
<b>Determination:</b>	<div><input type="checkbox"/> PTA sufficient at this time. <input type="checkbox"/> Privacy compliance documentation determination in progress. <input type="checkbox"/> New information sharing arrangement is required. <input type="checkbox"/> DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. <input type="checkbox"/> Privacy Act Statement required. <input checked="" type="checkbox"/> Privacy Impact Assessment (PIA) required. <input checked="" type="checkbox"/> System of Records Notice (SORN) required. <input type="checkbox"/> Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer. <input type="checkbox"/> A Records Schedule may be required. Contact your component Records Officer.</div>
<b>PIA:</b>	<b>System covered by existing PIA</b> If covered by existing PIA, please list: DHS/CBP/PIA-006(b) Automated Targeting System (ATS) DHS/CBP/PIA-007(g) Electronic System for Travel Authorization (ESTA)
<b>SORN:</b>	<b>System covered by existing SORN</b> If covered by existing SORN, please list: DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297





	DHS/CBP-009 Electronic System for Travel Authorization, September 2, 2016, 81 FR 60713
<b>DHS Privacy Office Comments:</b> <i>Please describe rationale for privacy compliance determination above.</i>	
<p>CBP is submitting this PTA to discuss the next update for the ESTA Social Media Pilot. The next phase of this program will support the transition of the (b)(7)(E) (b)(7)(E) There will also be further testing of the capabilities of social media vetting tools.</p> <p>The collection of ESTA applicant information is covered by the DHS/CBP/PIA-007(g) ESTA and the DHS/CBP-009 ESTA SORN, which was recently updated to include social media identifiers, such as username(s) and platforms used.</p> <p>The Privacy Office agrees that coverage for this pilot is provided under DHS/CBP/PIA-006(b) ATS, which outlines CBP's use of decision support tools in order to compare traveler information against law enforcement, intelligence, and other enforcement data. Additionally, this PIA outlines the querying of publicly available information in support of the vetting process. The DHS Privacy Office also agrees that SORN coverage is provided by the DHS/CBP-006 ATS SORN, which notes that CBP collects information on individuals whom may be subject to closer questioning or examination upon arrival to or departure from the United States or who may require further examination, as well as those who may pose a risk to border security or public safety, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law.</p> <p>This phase of this pilot may include other social media tools. S&amp;T is required to complete a tool-specific PTA for any of these tools that are planned to be used.</p>	